

基于 BNAG 模型的脆弱性评估算法

王 辉, 娄亚龙, 戴田旺, 茹鑫鑫, 刘 琨

(河南理工大学 计算机科学与技术学院, 河南 焦作 454000)

摘 要: 为准确评估计算机网络的脆弱性, 结合贝叶斯网络与攻击图提出一种新的评估算法。构建攻击图模型 RSAG, 在消除攻击图中环路的基础上, 将模型转换成贝叶斯网络攻击图模型 BNAG, 引入节点攻击难度和节点状态变迁度量指标计算节点可达概率。实例分析结果表明, 该算法对网络脆弱性的评估结果真实有效, 能够体现每个节点被攻击的差异性, 并且对于混合结构攻击图的计算量较少, 可准确凸显混乱关系下漏洞的危害程度。

关键词: 攻击图; 贝叶斯网络; 状态变迁; 可达概率; 脆弱性

开放科学(资源服务)标志码(OSID):



中文引用格式: 王辉, 娄亚龙, 戴田旺, 等. 基于 BNAG 模型的脆弱性评估算法[J]. 计算机工程, 2019, 45(9): 128-135, 142.

英文引用格式: WANG Hui, LOU Yalong, DAI Tianwang, et al. Vulnerability evaluation algorithm based on BNAG model[J]. Computer Engineering, 2019, 45(9): 128-135, 142.

Vulnerability Evaluation Algorithm Based on BNAG Model

WANG Hui, LOU Yalong, DAI Tianwang, RU Xinxin, LIU Kun

(School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan 454000, China)

[Abstract] In order to accurately evaluate the vulnerability of computer network, a new evaluation algorithm is proposed by combining Bayesian network with attack graph. An attack graph model is constructed, which is named RSAG. On the basis of eliminating the loop in the attack graph, the model is transformed into a Bayesian network attack graph model, which is named BNAG, and the node accessibility probability is calculated by introducing the node attack difficulty and node state transition measurement index. The analysis results of an example show that the evaluation results of network vulnerability by this algorithm are true and effective, which can fully reflect the difference between attacked node. Meanwhile, the calculation of attack graph with mixed structure is less, which can accurately highlight the harm degree of vulnerability in the chaotic relationship.

[Key words] attack graph; Bayesian network; state accessibility; accessibility probability; vulnerability

DOI: 10.19678/j.issn.1000-3428.0052317

0 概述

计算机网络在改变人们生产和生活方式的同时, 也面临着各类网络攻击。其中, 大部分的网络攻击都具有较强的传染性和破坏性, 会给社会以及计算机网络的安全带来较大的危害^[1]。根据中国互联网协会发布的《中国互联网站发展状况及其安全报告(2017)》^[2]可知, 截至 2016 年年底, 国家互联网应急中心 CNCERT 共发现 2 526 台服务器攻击并控制了 125.4 万台物联网智能设备, 对计算机网络的安全形成了严重的威胁。

近年来, 研究人员将贝叶斯网络和攻击图相结合^[3], 提出了风险管理框架^[4]、安全威胁识别及分析方法^[5]和混合路径攻击图模型^[6]等, 并引入贝叶斯概率来评估攻击图的脆弱性。相对于攻击图, 贝叶斯网络具备处理非确定性关系的能力, 而且能够量化攻击图中的对应关系。因此, 如何在网络脆弱性评估中将贝叶斯网络和攻击图更好地相结合, 是目前亟待解决的问题。

本文提出一种基于 BNAG 模型的脆弱性评估算法。在资源状态攻击图模型 RSAG 中引入贝叶斯概

基金项目: 国家自然科学基金(61300216)。

作者简介: 王 辉(1975—), 男, 副教授、博士, 主研方向为网络安全; 娄亚龙、戴田旺、茹鑫鑫, 硕士研究生; 刘 琨(通信作者), 副教授。

收稿日期: 2018-08-06 **修回日期:** 2018-09-26 **E-mail:** 892825026@qq.com

率,将其转换成贝叶斯网络攻击图模型BNAG,并通过节点攻击难度、节点状态变迁等指标计算各节点的可达概率,得到网络中各攻击路径的最终可达概率,从而提高对网络安全评估的有效性。

1 相关研究

近年来,众多学者运用攻击图技术分析网络的脆弱性。文献[7]分析状态攻击图、属性攻击图和贝叶斯攻击图的基本构成,同时阐述攻击图技术的研究现状,介绍几种攻击图的生成方法和分析工具。虽然文中指出了现有攻击图技术面临的挑战,但并未给出具体的解决方法。

文献[8]构建一种基于贝叶斯攻击图的动态风险评估模型,利用公共漏洞评分系统的索引计算攻击者成功执行的漏洞概率,通过引入局部条件概率表评估属性节点的静态安全风险。在此基础上,结合入侵检测系统观察到的实时攻击事件,利用贝叶斯推理预测攻击行为,动态计算后验概率。但该模型在计算节点概率时考虑的节点属性单一,得到的最大累积概率路径参考价值较小。

文献[9]提出基于推理规则的攻击图构建和分析技术,运用推理规则组合推算出新的攻击,从而做出对攻击图脆弱性的评估。但该文在实验中未考虑具体的度量值,准确率较低。

文献[10]建立一个面向内部攻击意图推断的概率攻击图模型,并在其中引入了转移概率表来刻画单步攻击的结果,在推测攻击意图的过程中设计一种推断内部攻击的算法和攻击路径最大概率的计算方法。但该文在进行路径分析及攻击意图推测时,未考虑节点间状态转移的影响。

文献[11]提出一种基于风险流攻击图的风险评估方法,采用攻击图来描述网络和攻击场景,然后将这些场景输入到网络流模型中。但该文未提及成本和转移概率等因素对网络脆弱性评估的影响。

文献[12]建立针对内部威胁的贝叶斯网络攻击图模型,在分析攻击行为时将似然加权法作为评估抽样的方法对内部威胁进行预测分析。但该文未考虑内部节点间的互相影响。

文献[13]依据要素之间的融合来评估攻击事件进行中攻击者的能力和漏洞利用率,设计基于动态贝叶斯攻击图的攻击预测算法,但在实验中并未考虑节点间状态转移的影响。

文献[14]构建一种可扩展的风险攻击图模型,给出全新的以风险流为对象的模糊风险评估机制,

以及面向组合漏洞攻击的基于人工免疫的多目标风险评估方法,但未提及因素之间的互相影响的问题。

本文把贝叶斯概率引入资源状态攻击图模型RSAG中,将其转换成贝叶斯网络攻击图模型BNAG,通过引入节点攻击难度、节点状态变迁等指标计算各节点的可达概率,得到网络中各攻击路径的最终可达概率。

2 资源状态攻击图模型

攻击图技术是根据网络状态和脆弱性信息,分析出攻击者在攻击网络时对网络脆弱性的利用序列,并将这些序列组成一张有向图。本文构造资源状态攻击图的目的是找出网络中存在的攻击序列,并通过贝叶斯概率计算推测出攻击者的意图,帮助网络管理人员更好地了解网络安全状况。本文构造的资源状态攻击图模型如下:

定义1 资源状态攻击图

资源状态攻击图 $RSAG = (S, S_0, A, E, \Gamma, L, O)$

是一个有向图,其中:

1) $S = \{s_i | i = 1, 2, \dots, N\}$ 表示资源状态节点集合。

2) $S_0 \in S$ 表示资源状态节点的初始状态,即最初攻击者占有的资源。

3) $A = \{a_i | i = 1, 2, \dots, N\}$ 表示攻击行为节点集合。

4) $E = \{E_1 \cup E_2\}$ 表示为连接各节点的有向边集合。

5) $E_1 \subseteq S \times A$ 表示只有当攻击者占有某些资源,攻击行为才能发生; $E_2 \subseteq A \times S$ 表示攻击行为可能使攻击者占有某些资源;通常节点 m 的父节点集合表示为 $Pre(m)$, 节点 m 的孩子节点集合表示为 $Nex(m)$ 。

6) Γ 表示节点状态判断函数。函数 $\Gamma(x)$ 代表节点的当前状态, $\Gamma(x) \in \{1, 0\}$ 。其中, $\Gamma(s_i)$ 代表资源状态节点的当前状态, $\Gamma(s_i) = 1$ 表示当前攻击者已经占有资源 s_i ; $\Gamma(a_i)$ 代表攻击行为节点的当前状态, $\Gamma(a_i) = 1$ 表示攻击行为 a_i 已经发生,反之则没有。

7) L 表示父节点之间的逻辑关系集。 $L = \{AND, OR, BLE\}$, 攻击行为节点 a_i 的前提条件全部满足后,攻击行为 a_i 才可能发生,所以 $Pre(a_i)$ 之间存在 AND 关系;任何攻击行为成功后都会使 $\Gamma(s_i) = 1$,即攻击者已占有资源 s_i ,所以当资源状态节点 s_i 作为 2 个或 2 个以上攻击行为的孩子节点时,这些攻击行为节点之间存在 OR 的关系;BLE 是指父节点之间的混乱逻辑关系。

8) $O = \{o_i | i = 1, 2, \dots, N\}$ 表示已经监测到攻击成功的资源状态节点集。对于 $\forall o_i \in S$, o_i 表示攻击行为 a_i 发生时被人侵检测系统观测到的攻击事件。

定义 2 攻击路径

在资源状态攻击图中,若存在一组状态序列 $s_0, a_0, s_1, a_1, \dots, a_{n-1}, s_n$ (s_0 是初始资源状态节点, s_n 是目标资源状态节点), 则定义攻击路径 $Path_k = \langle s_0 \rightarrow a_0 \rightarrow s_1 \rightarrow a_1 \rightarrow \dots \rightarrow a_{n-1} \rightarrow s_n \rangle$ 。其中: $\forall s_i \in S, \forall a_j \in A (0 \leq i \leq n, 0 \leq j \leq n-1)$; $Path_k$ 表示攻击图中第 k 条攻击路径。

定义 3 攻击行为

攻击行为用如下四元组表示: $(Src_id, Dst_id, Add_code, Res)$ 。其中, Src_id 是发动攻击的主机 id, Dst_id 是遭受攻击的主机 id, Add_code 是攻击行为编号, Res 此次攻击的结果。

定义 4 状态变迁

在攻击图中,状态变迁用三元组 (sid, vid, r) 表示。其中, sid 是状态变迁编号, vid 是攻击行为利用的脆弱点编号, r 是攻击行为利用脆弱点造成的状态变迁结果。

3 环路消除 E-Loop 算法

3.1 度量指标及计算方法

为消除攻击图中的环路,本文引入攻击难度度量指标,并给出相应的计算方法。在脆弱性评分系统 CVSS^[15] 中用访问矢量、访问复杂度和认证 3 个指标来描述脆弱点的可用性,本文分别用 Acc_vec 、 Acc_com 和 $Auth$ 来表示。3 个指标的度量等级如表 1 所示。

表 1 攻击难度度量等级

指标	低值	中值	高值
Acc_vec	0.359	0.646	1.000
Acc_com	0.350	0.610	0.710
$Auth$	0.450	0.560	0.704

CVSS 中脆弱点的可用性指标定义为:

$$Exp = 20 \times Acc_vec \times Acc_com \times Auth, 0 \leq Exp \leq 10 \quad (1)$$

Exp 的值越小,表示攻击行为发生的难度越大。因为可用性与攻击难度成反比,所以可以根据这 3 个指标计算节点的攻击难度。用 Aga_Dif 表示节点攻击难度度量指标, Aga_Dif 值越大,攻击难度越大,由此可判断出最难攻击节点,计算公式为:

$$Aga_Dif = \frac{1}{2 \times Acc_vec \times Acc_com \times Auth}, Aga_Dif \geq 1 \quad (2)$$

3.2 环路消除算法

在资源状态攻击图的生成中,会有出现环路的情况,导致遍历节点时重复,对网络安全评估尤其是贝叶斯概率计算造成很大影响。为解决这一问题,本文提出了 E-Loop 算法用于消除资源状态攻击图

RSAG 中的环路,算法具体步骤如下:

算法 1 环路消除算法 E-Loop(RSAG)

输入 资源状态攻击图 RSAG

输出 无环资源状态攻击图 Ac_RSAG

步骤 1 将攻击图的开始节点加入到根节点队列中。

步骤 2 初始化一个堆栈来存放找到的环路 $Init()$ 。

步骤 3 从入口节点开始进行深度优先遍历,依次访问各个节点 $root = GetRoot()$ 。

步骤 4 把访问节点压入到堆栈中,进行以下操作: $PushStack(root)$, 直到遍历完所有节点或者堆栈中已经存在遍历到的节点,此时堆栈中已经存储了一个环路。

步骤 5 计算环路中各节点的攻击度量 Aga_Dif_i , 找出最难攻击节点 $S_m = \max(Aga_Dif_i)$ 。

步骤 6 删除节点消除环路 $Delete(S_m)$ 。

步骤 7 重复步骤 3 ~ 步骤 6, 直到所测攻击图中不存在环路。

步骤 8 输出无环资源状态攻击图 Ac_RSAG。

图 1 是根据上述模型搭建的资源状态攻击图 RSAG。其中存在 $Path1 = \langle s_2 \rightarrow a_3 \rightarrow s_5 \rightarrow a_5 \rightarrow s_2 \rangle$ 和 $Path2 = \langle a_9 \rightarrow s_{11} \rightarrow a_{12} \rightarrow s_{12} \rightarrow a_9 \rangle$ 两条环路。对于 $Path1$, 通过 E-Loop 算法可去除节点 a_5 达到消除环路的目的; 对于 $Path2$, 因为 a_9 节点永远无法到达, 其 $Aga_Dif(a_9) \rightarrow \infty$, 所以去除 a_9 节点达到消除环路的目的。图 2 是用 E-Loop 算法消除环路后的无环资源状态攻击图 Ac_RSAG。

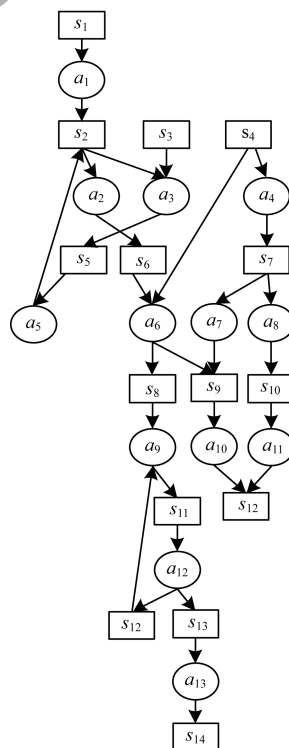


图 1 资源状态攻击图 RSAG

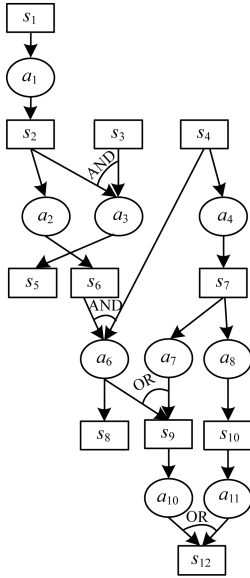


图 2 无环资源状态攻击图 Ac_RSAG

4 基于 BNAG 模型的可达概率计算

在贝叶斯网络中,节点的概率只与其父节点有关,与其他节点保持条件独立。在资源状态攻击图中状态的转移只与相应的资源是否被占用有关,且父节点的资源被占用是状态变迁到子节点的必要条件。因此,可以将无环资源状态攻击图中的状态转移过程与贝叶斯网络中的条件独立性相对应。表 2 给出了无环资源状态攻击图 Ac_RSAG 与贝叶斯网络攻击图 BNAG 结构上的对应关系。

表 2 攻击图与贝叶斯网络对应关系

比较项目	Ac_RSAG	BNAG
图类型	有向无环图	有向无环图
节点关系	脆弱性与状态变迁存在因果关系	因果关系网络
节点类型	网络状态节点	网络节点
连接关系	占用节点资源的攻击行为过程	节点之间的有向边
变迁关系	状态发生变迁的概率	节点之间条件概率
依赖关系	节点的状态变迁与非父节点无关	节点的条件独立性

无环资源状态攻击图 Ac_RSAG 和贝叶斯网络攻击图 BNAG 虽然在结构上有所对应,但具体到各个节点仍存在差异,下文将给出贝叶斯网络攻击图 BNAG 的具体实现方法。

4.1 贝叶斯网络攻击图 BNAG 的实现

定义 5 条件资源状态节点和结果资源状态节点:为满足攻击行为发生的条件,所需要的资源状态节点称为条件资源状态节点;攻击行为到达的资源状态节点称为结果资源状态节点。

定义 6 $W = \{w_{ij} | i, j = 1, 2, \dots, N\}$ 表示资源状态节点之间的权重集,其由二元组 $(depcoef, cost)$ 表示,其中: $depcoef$ 表示资源状态节点间的关联程度系数; $cost$ 表示从一个资源状态节点到另一个资源

状态节点攻击花费的代价; w_{ij} 表示资源状态节点 s_i 和 s_j 之间有向边的权重。

如图 2 所示,资源状态攻击图包含 4 种基本结构,分别是串联结构、并联 AND 结构、并联 OR 结构和混合结构。在转化为贝叶斯网络攻击图 BNAG 时,对各结构的处理方法如下:

1) 串联结构:把攻击行为节点删除,用资源状态节点 s_1 到资源状态节点 s_2 的有向边表示攻击行为,具体表示为: $(s_1 \rightarrow a_1 \rightarrow s_2) \Rightarrow (s_1 \rightarrow s_2)$ 。

2) 并联 AND 结构:攻击行为节点 a_3 的父节点 s_2 和 s_3 之间是 AND 关系,只有当资源状态全部满足时攻击行为才会发生。将攻击行为节点删除,条件资源状态节点和结果资源状态节点之间用 1 条有向边连接,用该有向边表示攻击行为。转换后的贝叶斯网络攻击图中,资源状态节点之间仍为 AND 关系,具体表示为: $(s_2 \wedge s_3 \rightarrow a_3 \rightarrow s_5) \Rightarrow (s_2 \wedge s_3 \rightarrow s_5)$ 。

3) 并联 OR 结构:攻击行为节点 a_{10} 和 a_{11} 之间是 OR 关系,攻击行为节点的父节点 s_9 和 s_{10} 中只要有一个满足,攻击行为就会发生。将攻击行为节点删除,将条件资源状态节点和结果资源状态节点之间用有向边连接。转换后在贝叶斯网络攻击图中,资源状态节点之间仍为 OR 关系: $(s_9 \rightarrow a_{10}, s_{10} \rightarrow a_{11}, a_{10} \vee a_{11} \rightarrow s_{12}) \Rightarrow (s_9 \vee s_{10} \rightarrow s_{12})$ 。

4) 混合结构:攻击行为节点 a_6 的父节点 s_6 和 s_4 之间是 AND 关系,到达结果资源状态节点的 2 个攻击行为节点 a_6 和 a_7 之间是 OR 关系,如果直接删除攻击行为节点 a_6 ,会造成资源状态攻击图的结构混乱,不利于条件概率的计算。为解决此问题,本文引入一个临时混合节点 $blend$,即把 a_6 节点抽象为一个临时混合节点 $blend$,具体表示为: $(s_6 \wedge s_4 \rightarrow a_6, a_6 \vee a_7 \rightarrow s_9) \Rightarrow (s_6 \wedge s_4 \rightarrow blend, blend \vee s_7 \rightarrow s_9)$ 。

在攻击图转换过程中,因为每条边代表了攻击行为,所以在转换后的贝叶斯网络攻击图中每条边都有一个权重 W ,用于描述 2 个资源状态节点关联关系。转换后的贝叶斯网络攻击图 BNAG 如图 3 所示。

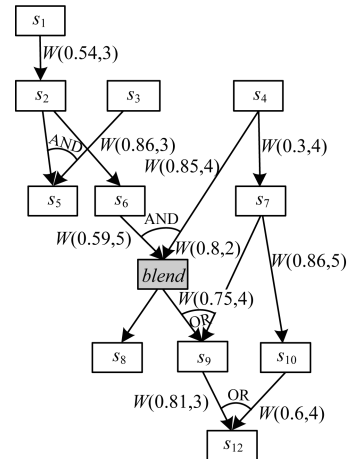


图 3 贝叶斯网络攻击图 BNAG

由转化后的贝叶斯网络攻击图可知, $blend$ 是 s_4 和 s_6 的混合资源状态, 则 s_4 和 s_6 到 $blend$ 的有向边一定成立, 即 $P(blend | s_4, s_6) = 1$ 。因此, 转化为贝叶斯网络后各节点之间的关系不会改变, 且其中只含有资源状态节点, 攻击行为体现在贝叶斯网络攻击图的有向边上, 有向边之间只有 AND 和 OR 的关系。为了更清楚地描述转换的过程, 本文设计攻击图转换算法 Alg-AGTrans, 具体描述如下:

算法 2 攻击图转换算法 Alg-AGTrans(RSAG)

输入 无环资源状态攻击图 Ac_RSAG

输出 贝叶斯网络攻击图 BNAG

1. For each $s_i \in S$ AND $a_i \in A$
2. If $DPre(s_i) \neq \emptyset$ AND IF $DPre(a_i) \neq \emptyset$
3. Else If $Num(DPre(a_i)) = 1$ AND
 $Num(DPre(DNex(a_i))) = 1$
4. $e_{ij} = \langle s_i, DNex(a_i) \rangle$;
5. $e_{ij} \leftarrow W(i, j)$;
6. Delete(a_i); //删除攻击行为节点
7. Else If $Num(DPre(a_i)) > 1$
8. $e_{ij} = \langle DPre(a_i), DNex(a_i) \rangle$;
9. $e_{ij} \leftarrow W(i, j)$;
10. Delete(a_i);
11. $\forall e_{ij}$ -之间都是 AND 关系;
12. Else If $Num(DPre(s_i)) > 1$
13. $e_{ij} = \langle DPre(DPre(s_i)), s_i \rangle$;
14. $e_{ij} \leftarrow W(i, j)$;
15. Delete($DPre(s_i)$);
16. $\forall e_{ij}$ -之间都是 OR 关系;
17. Else If $DPre(a_i) > 1$ AND $Num(DPre(Nex(a_i))) > 1$
18. $a_i \in Ble$; $a_i = blend$;
19. $e_{ij} = \langle DPre(blend), blend \rangle$;
20. $e_{ij} \leftarrow W(i, j)$;
21. $\forall e_{ij}$ -之间都是 AND 关系;
22. $e_{ij} = \langle blend, DNex(blend) \rangle$;
23. $e_{ij} \leftarrow W(i, j)$;
24. $\forall e_{ij}$ -之间都是 OR 关系;
25. End If;
26. Go to For;
27. Return BNAG;

4.2 基于 BNAG 的节点可达概率计算

本文定义节点 S 的直接父节点为 $DPre(S)$, 根据贝叶斯网络中节点间概率的独立性可以得出目标所受到攻击的概率 $P_a(S)$ 为:

$$P_a(S) = P(S | Pre(S)) P(Pre(S)) = P(S | DPre(S)) P(DPre(S)) \quad (3)$$

状态变迁指标 $P_m(cost_i)$ 定义为状态 S_{i-1} 变迁到状态 S_i 的概率。因为资源状态节点与其父节点之间

存在关联, 所以在计算其状态变迁指标时需要把节点间的权重 W 考虑进去。如果花费足够的代价, 其攻击目的一定能达到, 即当 $cost \rightarrow \infty$ 时, $P_m(cost) = 1$; 若不付出任何代价, 其不可能成功攻击任一目标, 即当 $cost = 0$ 时, $P_m(cost) = 0$; 若对应节点攻击没有成功, 节点的状态保持不变。状态变迁指标 $P_m(cost_i)$ 的取值符合指数分布的特点。所以, 定义 $P_m(cost_i)$ 的计算公式如式(4)所示。

$$P_m(cost_i) = P(cost_i < cost) = 1 - e^{-depcoef \times cost_i} \quad (4)$$

其中: $cost_i$ 是攻击所花费的代价, 指攻击者完成一次攻击所需要花费的经验知识和所需要的资源权限等; $cost$ 为完成最后目标攻击后总的平均攻击代价, 是一个预设值, 平均攻击代价取决于攻击者的知识水平、利用资源、攻击时间和工具等; $depcoef$ 是资源状态节点间的关联程度系数, 计算公式如式(5)所示。

$$depcoef = \frac{1}{Aga_Dif}, 0 < depcoef < 1 \quad (5)$$

因此, 状态变迁指标 $P_m(cost_i)$ 的计算公式如下:

$$P_m(cost_i) = 1 - e^{-\frac{cost_i}{Aga_Dif}} \quad (6)$$

由上文可知, 贝叶斯网络攻击图中资源状态节点间存在相互影响关系, 在进行攻击图脆弱性分析时, 不能仅通过传统的贝叶斯推理对节点可达概率进行分析, 还应该考虑节点间状态变迁。为解决该问题, 本文在此基础上引入状态变迁指标, 在脆弱性研究的过程中加入对节点的状态变迁的考虑。定义 P_{end} 表示目标节点可达概率, 计算公式如式(7)所示。

$$P_{end}(s_i) = P_m(cost_i) \times P_a(s_i) = (1 - e^{-\frac{cost_i}{Aga_Dif}}) \times P(s_i | DPre(s_i)) P(DPre(s_i)) \quad (7)$$

其中: $P_m(cost_i)$ 为目标节点 s_i 状态变迁的指标, $depcoef$ 为节点 s_i 与其直接父节点的关联程度系数; $cost$ 为从节点 s_i 到下一个节点攻击所花费的代价; $P_a(s_i)$ 为目标节点 s_i 所受到攻击的贝叶斯概率。

式(7)为目标节点可达概率的计算方法, 迭代式(7)就可以得出整条路径的可达概率。迭代算法 IterAlg-AccPro 具体描述如下:

算法 3 迭代算法 IterAlg-AccPro(BNAG, W)

输入 转换后的贝叶斯网络攻击图 BNAG, 节点间的权重 $W = (depcoef, cost)$

输出 整条路径下最终攻击可达概率 $P_{end}(s_i)$

1. For each $s_i \in S$
2. Count = $DPre(s_i)$ 的数目;
3. InitStack(&q); //构造一个空栈, 用于存储父节点

4. For each $DPre(s_i) \in S$ and $DPre(s_i) \neq \emptyset$
5. $root = DPre(s_i)$; // 获取目标节点的直接父节点
6. $PushStack(root) \rightarrow q$; // 把目标节点的父节点压入栈 q
7. End for
8. End for
9. For $q \neq \emptyset$
10. $s_i = PopStack(root)$; // 从栈中取出节点元素
11. $P_a = P_a(s_i)$;
12. $P_a = P_a(cost_{dpre(s_i)})$;
13. $P_{end} = P_a \times P_m$;
14. End for;
15. Return P_{end} ;

IterAlg-AccPro 算法首先遍历了所有节点, 根据目标节点 s_i 的直接父节点 $DPre(s_i)$ 的个数, 把所有的父节点 $Pre(s_i)$ 依次压入到各自的堆栈 q 中, 保证每个直接父节点 $DPre(s_i)$ 所在路径的开始节点最后压入堆栈; 然后利用堆栈后进先出的特点依次取出其中的节点并计算其可达概率; 最后得出整条路径的可达概率。在计算中引入节点间的状态变迁指标, 提高了计算效率和准确性。

假设要攻击的节点为 s_{12} , 由图 3 可知共有 3 条攻击路径可以到达攻击目标, 分别为:

- Path1: $\langle s_1 \rightarrow s_2 \rightarrow s_6 \rightarrow blend(s_6 \wedge s_4) \rightarrow s_9 \rightarrow s_{12} \rangle$
 Path2: $\langle s_4 \rightarrow s_7 \rightarrow s_9 \rightarrow s_{12} \rangle$
 Path3: $\langle s_4 \rightarrow s_7 \rightarrow s_{10} \rightarrow s_{12} \rangle$

若考虑节点间的权重 W , 其中资源状态节点间关联程度系数 $depcoef$ 和攻击花费代价 $cost_i$ 的取值以图 3 标注为准, s_1 、 s_4 的先验概率为 0.2、0.3。以路径 Path1 为例, 具体的运算步骤如下:

$$\begin{aligned}
 P(s_2) &= P_m(cost_1) \times P(\Gamma(s_2) = 1 | \Gamma(s_1) = 1) \times \\
 &P(s_1) = 0.0866 \\
 P(s_6) &= P_m(cost_2) \times P(\Gamma(s_6) = 1 | \Gamma(s_2) = 1) \times \\
 &P(s_2) = 0.0684 \\
 P(blend) &= P_m(cost_6) \times P(\Gamma(blend) = \\
 &1 | \Gamma(s_6) = 1, \Gamma(s_4) = 1) \times \\
 &P(s_6) \times P(s_4) = 0.0382
 \end{aligned}$$

同理, 通过式 (7) 可依次得到: 路径 Path1 下攻击者到达 s_9 、 s_{12} 的概率分别为 $P(s_9) = 0.0272$ 和 $P_{end}(s_{12}) = 0.0201$; 路径 Path2 下攻击者到达 s_{12} 的概率为 $P_{end}(s_{12}) = 0.0648$; 路径 Path3 下攻击者到达 s_{12} 的概率为 $P_{end}(s_{12}) = 0.0573$ 。如果管理员已经知道 a_1 已经被攻击, 即 $P(s_1) = 1$, 则再次计算路径 Path1 下攻击者到达 s_{12} 的概率 $P_{end}(s_{12}) = 0.0631$, 因此, 当资源状态 s_1 确定满足后, s_{12} 受到攻击的概率明显增大, 与预期的结果一致。

5 实验与结果分析

5.1 实验网络环境

为了验证本文方法的可行性和有效性, 笔者在研究河南理工大学校园网的基础上搭建了如图 4 所示的实验环境, 其中主机与服务器均有多台, 在模拟仿真实验网络拓扑图中只列出具有代表性的服务器和主机。

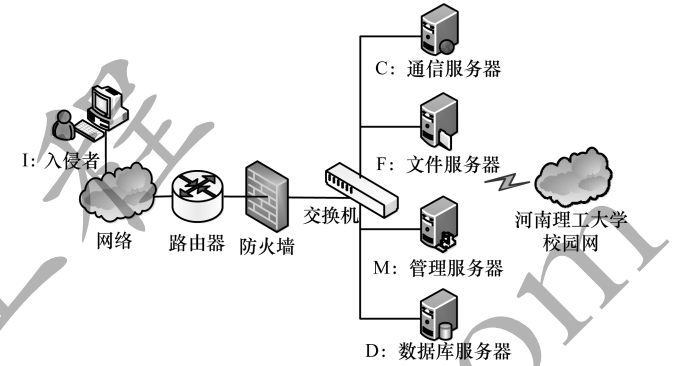


图 4 实验网络拓扑

实验网络中共有 5 台主机, 分别是入侵者机器、通信服务器、文件服务器、管理服务器、数据库服务器。为了方便描述, 分别用字母 I、C、F、M 和 D 表示。其中: 通信服务器 C 开放了 Telnet 服务; 文件服务器 F 开放了 FTP 服务; 管理服务器 M 开放了 FTP 和 HTTP 服务; 数据库服务器 D 开放为 Oracle 服务; 入侵者 I 的最终目的是要获得主机 D 的 root 权限, 防火墙只允许外部主机 I 访问主机 C 上的 Telnet 服务, 其他的外部访问均被阻止; 内部主机只允许主机 M 访问主机 D 上的 Oracle 服务, 其他 3 个主机之间可以互相访问; 主机 C 直接访问主机 M, 且同时获取了主机 M 开放的 2 个服务的访问权限时, 主机 C 就可以通过这 2 个服务直接访问主机 D 上的 Oracle 服务。内部主机信息如表 3 所示。

表 3 内部主机信息

主机标识	开放服务	脆弱性编号
C	{Telnet}	{12 815}
F	{FTP}	{9 904, 13 454}
M	{FTP, HTTP}	{7 974, 8 952}
D	{Oracle}	{14 312}

5.2 结果分析

根据本文的攻击图模型和实验网络拓扑图, 在生成资源状态攻击图的过程中, 通过 E-Loop 算法去除环路后, 存在的攻击行为节点对应的攻击行为编号 Att_code 如表 4 所示, 其与主机开放的服务和脆弱性编号有关。

表 4 攻击图实例中攻击行为信息

vid	Src_id	Att_code	Dst_id	Res
12 815	I	tel-rsh(I,C)	C	Trust(C,I)
9 904	C	ftp-rhost1(C,F)	F	Trust1(F,C)
13 454	C	ftp-rhost2(C,F)	F	Trust2(F,C)
7 974	F,C	ftp-rhost(F,M), ftp-rhost(C,M)	M	Trust1(M,F) Trust1(M,C)
8 952	F,C	http-rsh(F,M), http-rsh(C,M)	M	Trust2(M,F) Trust2(M,W)
14 312	M	oracle(M,D), oracle(C,D)	D	Trust(D,M), Trust(D,C)

在实验网络拓扑图的基础上,利用攻击图转换算法 Alg-AGTrans 消去表 4 中的攻击行为节点后,得到的贝叶斯网络攻击图如图 5 所示。

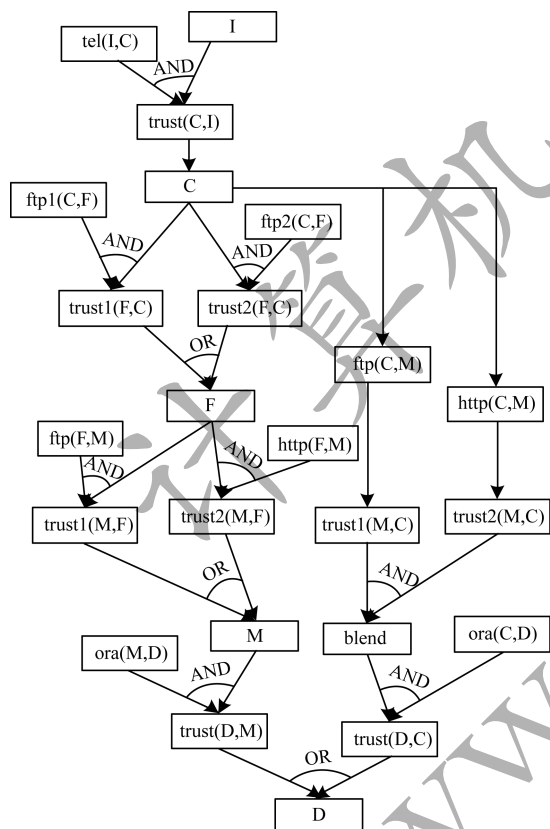


图 5 贝叶斯网络攻击图

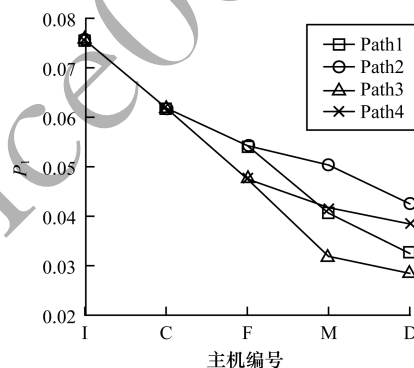
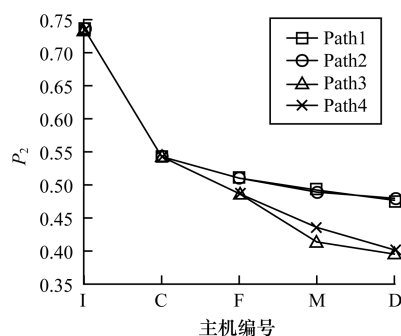
如图 5 所示,贝叶斯网络攻击图实例中,各主机节点必须通过另外一台主机开放的服务来获取其信任,所以在结构上是 AND 关系;当一台主机开放 2 个服务时,获取其中一个服务的权限就可以得到该主机的信任,因此其攻击主机之间是 OR 关系;特殊情况下的混合关系节点,是攻击主机同时获取到目标主机开放的 2 个服务时,就可以直接越过该主机直接访问下一个主机开放的服务,在此引入 blend 节点来处理攻击图实例中的混乱关系。

图 5 中的路径可到达目标主机 D,其攻击路径信息和路径可达概率如表 5 所示。其中:Src_id 是攻击者主机;Dst_id And Service 是被攻击主机 id 和被利用的漏洞编号;Len 是攻击路径总长度; P_1 是根据本文提出的算法引入状态变迁指标后得出的整条路径的可达概率; P_2 是未引入状态变迁指标时得出的整条路径的可达概率。

表 5 实例图攻击路径信息

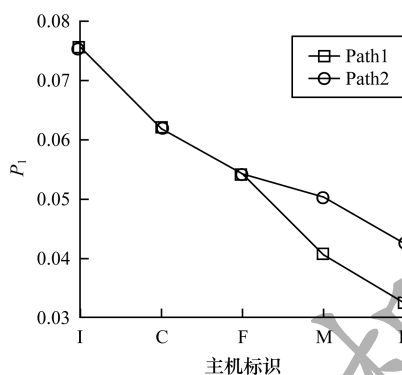
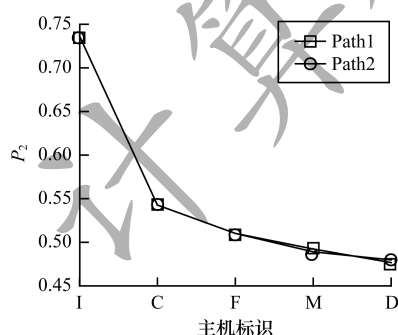
路径	Src_id	Dst_id And Service	Len	P_1	P_2
Path1	I	(C:12 815) (F:9 940) (M:7 974) (D:14 312)	9	0.032 47	0.476 8
Path2	I	(C:12 815) (F:9 940) (M:8 952) (D:14 312)	9	0.042 52	0.478 9
Path3	I	(C:12 815) (F:13 454) (M:7 974) (D:14 312)	9	0.028 46	0.395 4
Path4	I	(C:12 815) (F:13 454) (M:8 952) (D:14 312)	9	0.038 45	0.401 8
Path5	I	(C:12 815) (M:7 974,8 952) (D:14 312)	8	0.048 36	0.391 2

在表 5 的基础上,本文给出每个主机节点的可达概率,具体的概率分布如图 6、图 7 所示。

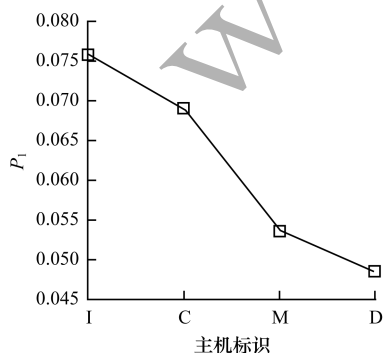
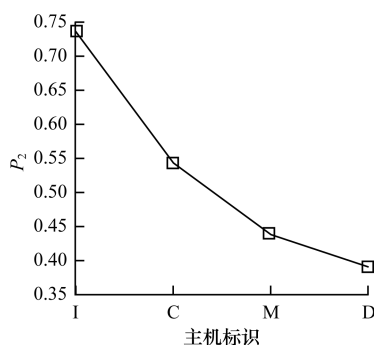
图 6 P_1 下 Path1 ~ Path4 概率图 7 P_2 下 Path1 ~ Path4 概率

如图 8、图 9 所示,对于 Path1 和 Path2 路径,其路径中攻击主机都相同,唯一的区别是访问主机 M 的服务不同,Path1 访问的是主机 M 的 ftp 服务,

Path2 访问的是主机 M 的 http 服务。通过本文提出的算法引入状态变迁指标后计算得到的 Path1 和 Path2 的最终路径可达概率为 0.032 47 和 0.057 84, 在主机 F 到主机 M 上有明显的变化, 如图 8 所示; 而对于未引入状态变迁指标的方法计算 Path1 和 Path2 最终路径的可达概率分别为 0.476 8 和 0.478 9, 在主机 F 到主机 M 没有明显变化, 如图 9 所示。本文算法虽然使单个节点的概率参考值变小, 但充分体现了攻击每个节点时的差异性, 更利于网络安全管理员的分析。

图8 P_1 下 Path1、Path2 概率图9 P_2 下 Path1、Path2 概率

如图 10、图 11 所示, 对于有混乱关系的路径 Path5, 传统的计算方法是把 AND 和 OR 节点分开计算来处理混乱关系, 不仅计算量大, 而且忽视了其中的关联关系, 本文引入混合节点的方法, 不仅减小了计算量, 而且计算结果具有更高的参考价值。

图10 P_1 下 Path5 概率图11 P_2 下 Path5 概率

对于主机 C 访问主机 M 时出现的混乱关系, 加入状态变迁指标后得到的概率分布更能凸显出混乱关系下漏洞的危害程度, 更能引起网络安全管理员的注意。

6 结束语

如何提高网络脆弱性评估的准确性是网络安全领域研究的热点。本文提出一种基于 BNAG 模型的脆弱性评估算法, 同时给出 E-Loop 算法用于消除攻击图中的环路。在贝叶斯网络攻击图 BNAG 的转换过程中, 设计 Alg-AGTrans 算法解决节点关系混乱的问题。本文在推导节点可达概率的计算公式时, 引入节点攻击难度指标和节点状态变迁指标, 提出 IterAlg-AccPro 算法。实验结果表明, 该算法对网络脆弱性的评估真实、有效, 但在计算节点可达概率时没有考虑到风险成本等因素的影响, 下一步将对此加以改进。

参考文献

- [1] 穆雪峰. 网络型病毒传播与计算机网络安全[J]. 信息与电脑(理论版), 2017(12): 200-202.
- [2] 中国互联网发展状况及其安全报告(2017)[EB/OL]. [2018-07-05]. <http://www.isc.org.cn/zxxz/xhdt/listinfo-35526.html>.
- [3] 李艳, 黄光球. 动态攻击网络演化分析模型[J]. 计算机应用研究, 2016, 33(1): 266-270.
- [4] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using Bayesian attack graphs[M]. Washington D.C., USA: IEEE Computer Society Press, 2012.
- [5] 吴迪, 连一峰, 陈恺, 等. 一种基于攻击图的安全威胁识别和分析方法[J]. 计算机学报, 2012, 35(9): 1938-1950.
- [6] 余洋, 夏春和, 胡潇云. 采用混和路径攻击图的防御方案生成方法[J]. 浙江大学学报(工学版), 2017, 51(9): 1745-1759.
- [7] 叶子维, 郭渊博, 王宸东, 等. 攻击图技术应用研究综述[J]. 通信学报, 2017, 38(11): 121-132.
- [8] 高妮, 高岭, 贺毅岳, 等. 基于贝叶斯攻击图的动态安全风险评估模型[J]. 四川大学学报(工程科学版), 2016, 48(1): 111-118.

(下转第 142 页)

(上接第 135 页)

- [9] KRAUTSEVICH L. Parametric attack graph construction and analysis[J]. *Organometallics*, 2015, 30(12): 98-101.
- [10] 陈小军, 方滨兴, 谭庆丰, 等. 基于概率攻击图的内部攻击意图推断算法研究[J]. *计算机学报*, 2014, 37(1): 62-72.
- [11] DAI Fangfang, HU Ying, ZHENG Kangfeng, et al. Exploring risk flow attack graph for security risk assessment[J]. *IET Information Security*, 2015, 9(6): 344-353.
- [12] 王辉, 亢凯航, 刘淑芬. 基于贝叶斯推理的 PASG 计算模型[J]. *计算机工程*, 2016, 42(11): 158-164.
- [13] 胡浩, 叶润国, 张红旗. 基于攻击预测的网络安全态势量化方法[J]. *通信学报*, 2017, 38(10): 122-134.
- [14] 戴方芳. 基于攻击图理论的网络安全风险评估技术研究[D]. 北京: 北京邮电大学, 2015.
- [15] TRIPATHI A, SINGH U K. Analyzing trends in vulnerability classes across CVSS metrics[J]. *International Journal of Computer Applications*, 2011(3): 38-40.

编辑 金胡考